НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___”_____20 _ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки : 113 «Прикладна математика»
(код і назва)

на тему: Диференціальні властивості ітеративних перетворень із залежними ключами _____
_____
_____

Виконав: студент 4 курсу, групи ФІ-62
(шифр групи)

Пясецький Богдан Юрійович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник Доцент кафедри ММЗІ, к.т.н. Яковлєв С. В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент Доцент кафедри ІБ, к.т.н. Стьопочкіна І. В. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут

Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки - 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою

М.М.Савчук

_____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту

Пясецькому Богдану Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Диференціальні властивості ітеративних перетворень із залежними ключами _____
_____
_____ ,
керівник роботи Доцент кафедри ММЗІ, к.т.н. Яковлєв С. В. _____ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____

4. Зміст роботи огляд опублікованих джерел за тематикою дослідження, дослідження поведінки імовірностей диференціалів для простого модельного шифру із однаковими раундовими ключами та лінійнозалежними раундовими ключами, дослідження поведінки лінійних потенціалів для наведеного модельного шифру _____
_____

_____

_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) презентація _____

_____

_____

_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Узгодження теми з науковим керівником	1 – 15 жовтня	Виконав
2	Аналіз опублікованих джерел за тематикою дослідження	16 – 20 жовтня	Виконав
3	Аналіз диференціальних властивостей ітеративного шифру з фіксованими ключами	1 листопада – 20 грудня	Виконав
4	Аналіз диференціальних властивостей ітеративного шифру із залежними ключами	21 грудня – 13 січня	Виконав
5	Аналіз лінійних потенціалів ітеративного шифру з фіксованими ключами	1 березня – 22 квітня	Виконав
6	Аналіз лінійних потенціалів ітеративного шифру із залежними ключами	23 квітня – 15 травня	Виконав
7	Оформлення пояснювальної записки до дипломної роботи	17 травня – 3 червня	Виконав

Студент _____ Пясецький Б. Ю.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Яковлєв С. В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Кваліфікаційна робота містить: 46 стор., 2 рисунки, 10 таблиць, 26 джерел.

Метою даної роботи є вдосконалення методів та уточнення формальної теорії диференціального та лінійного криптоаналізу на випадок залежних раундових ключів ітеративного блокового шифру. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження — криптографічні властивості ітеративних перетворень із залежними ключами.

Експериментально було показано, що перетворення із залежними раундовими ключами втрачають властивість марковості, однак для деяких форм раундової функції вони можуть зберігати окремі властивості модельних шифрів – зокрема, значення середніх імовірностей диференціалів. Було встановлено, що для деяких дворaундових функцій із простою структурою використання раундових ключів які, або співпадають, або є залежними один від одного дуже простим чином, погіршує стійкість до диференціального та лінійного криптоаналізу у порівнянні з ситуацією, коли два ключа є різними і незалежними.

ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, ЛІНІЙНИЙ КРИПТОАНАЛІЗ, МАРКОВСЬКІ ПЕРЕТВОРЕННЯ, РАУНДОВІ КЛЮЧІ

ABSTRACT

Qualification work contains: 46 pages, 2 drawings, 10 tables, 26 sources.

The purpose of this work is to improve the methods and clarify the formal theory of differential and linear cryptanalysis in cases of dependent round keys of iterative block cipher. The object of research is information processes in cryptographic protection systems. The subject of the study is the cryptographic properties of iterative mappings with dependent keys.

It has been shown experimentally that mappings with dependent round keys become non-Markov ciphers, but for some forms of the round function they can retain some properties of model ciphers - in particular, the values of the average probabilities of differentials. It was found that for some two-round functions with a simple structure the use of round keys, which either coincide or are dependent on each other in a very simple way, impairs the resistance to differential and linear cryptanalysis in comparison with the situation when round keya are different and independent.

DIFFERENTIAL CRYPTANALYSIS, LINEAR CRYPTANALYSIS, MARKOV CIPHERS, ROUND KEYS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

V_n — простір двійкових векторів довжини n: $V_n = \{0,1\}^n$

$\oplus$ — додавання за модулем 2

$[P]$ — дужки Айверсона: $[P]$ дорівнює 1, якщо P - істинне, та 0, якщо P - хибне

$\overline{\sum_x}$ – усереднена сума по всіх x

$a \to b$ — диференціал (a,b) деякої булевої функції

$DP^f_{\circ,\bullet}(a,b)$ — імовірність диференціалу (a,b) функції f із вхідною операцією $\circ$ та вихідною операцією $\bullet$

$MDP_{\circ,\bullet}(f)$ — максимальна диференціальна імовірність функції f

$EDP^{f_k}_{\circ,\bullet}(a,b)$ — середня імовірність диференціалу (a,b) параметризованої ключем функції f_k із вхідною операцією $\circ$ та вихідною операцією $\bullet$

$MEDP_{\circ,\bullet}(f_k)$ — максимальна середня диференціальна імовірність параметризованої ключем функції f_k

$DP^f_{\circ,\bullet}(x,a,b)$ — імовірність диференціалу (a,b) параметризованої ключем функції f_k із вхідною операцією $\circ$ та вихідною операцією $\bullet$ у точці x

$MDP_{\circ,\bullet}(f_k)$ — максимальна диференціальна імовірність параметризованої ключем функції f_k, враховуючи всі точки входу

DDT^F — таблиця розподілів диференціалів функції F

$\delta(F)$ — диференціальна рівномірність функції F

$\lambda_F(a,b)$ — коефіцієнт Уолша для функцції F

$LP^F(a,b)$ — лінійний потенціал функції F

$ELP^{F_k}(a,b)$ — середній за ключами лінійний потенціал функції F_k

$MELP(F_k)$ — максимальний середній за ключами лінійний потенціал функції F_k

ВСТУП

Актуальність дослідження. У диференціальному та лінійному криптоаналізі сучасних блокових шифрів використовують стандартне модельне припущення, що раундові ключі є випадковими, рівноімовірними та незалежними. Саме в рамках даного припущення і були побудовані теорії диференціального криптоаналізу та лінійного криптоаналізу. Користуючись цим припущенням Рюмен та Демен дослідили асимптотичні розподіли диференціальних імовірностей та лінійних потенціалів марковських шифрів із зафіксованими ключами та показали, що значення середніх імовірностей будуть параметрами відповідних граничних розподілів для імовірностей диференціалів таких перетворень. Але на практиці ключі не є випадковими та незалежними. Питання, наскільки працює дане модельне припущення у випадках, коли раундові ключі явно не є незалежними, залишається відкритим й досі.

В літературі дане питання досліджено дуже слабо. Один із випадків, коли раундові ключі є фіксованими, відповідно незалежними, був розглянутий Лі та Ванем, в результаті чого для 3-х раундів шифрування схемою Фейстеля із константними ключами були виведені нижні межі для диференціальної рівномірності та лінійності. А питання, коли раундові ключі є залежними, у відкритих джерелах майже не досліджено.

Метою дослідження є вдосконалення методів та уточнення формальної теорії диференціального та лінійного криптоаналізу на випадок залежних раундових ключів ітеративного блокового шифру. Для досягнення поставленої мети необхідно розв'язати такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити поведінку імовірностей диференціалів для простого модельного шифру з однаковими раундовими ключами та лінійно залежними раундовими ключами;

3) дослідити поведінку лінійних потенціалів для наведеного модельного шифру.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. *Предметом дослідження* є криптографічні властивості ітеративних перетворень із залежними ключами.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи теорії імовірностей, лінійна та абстрактна алгебра, комп'ютерне моделювання.

Наукова новизна отриманих результатів полягає в тому, що вперше було розглянуто поведінку параметрів стійкості до диференціального та лінійного криптоаналізу для ітеративних блокових шифрів із залежними ключами, і показано, що стандартне модельне припущення не завжди виконується коректно, а також, що істинна оцінка стійкості може відрізнятись в гірший бік, від тієї оцінки, яку надає теорія.

Практичне значення. Результати даної роботи можна використати для уточнення формальної теорії диференціального та лінійного криптоаналізу ітеративних блокових шифрів.

Апробація результатів та публікації. Частина результатів даної роботи було представлено на XVIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (12 – 13 травня 2020 року, м.Київ).

1 ІТЕРАТИВНІ БЛОЧНІ ШИФРИ ТА ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ

У даному розділі розглядаються, необхідні для нашого дослідження, теоретичні відомості з диференціального криптоаналізу, та основні поняття, які використовуються у лінійному криптоаналізі. Також будуть розглянуті роботи Рюмена та Демена в яких вони досліджували асимптотичний розподіл $(\oplus,\oplus)$-імовірностей при фіксованих ключах, і робота Канто та ін., яка бере за основу результати досліджень Лі та Ваня для 3-х раундовії схеми Фейстеля з однаковими ключами.

1.1 Основні поняття диференціального криптоаналізу. Марковські та немарковські перетворення

Нехай M — множина відкритих текстів, C — множина шифротекстів, K — множина ключів.

Означення 1.1. *Шифруюче перетворення* — це функція вигляду

$$f : M \times K \to C,$$

що задовольняє такій умові: для кожного фіксованого значення $k \in K$ перетворення $y = f(x,k)$ є бієктивним.

Часто для шифруючих перетворень замість позначення $f(x,k)$ використовують позначення $f_k(x)$, щоб підкреслити параметричну роль ключа. У випадках, коли ключ розглядається як випадкова величина (а шифруюче повідомлення, відповідно, як стохастична функція від ключа), може також використовуватись позначення $f[k](x)$.

Означення 1.2. *Диференціал булевої функції f відносно операцій* $(\circ,\bullet)$ (або просто $(\circ,\bullet)$ - *диференціал*) — це пара двійкових векторів (a,b),

для яких існує значення x, і при цьому виконується співвідношення:

$$f(x \circ a) \bullet (f(x))^{-1} = b$$

де через q^{-1} позначено обернений до q елемент відносно операції $\bullet$.

Параметр a будемо називати вхідною різницею, b — вихідною різницею, операцію $\circ$ — операцією різності на вході, $\bullet$ — операцією різності на виході. Часто диференціал може позначається символом $a \xrightarrow{f} b$ або $a \to b$, підрозуміваючи під цим, що вхідна різниця a під дією функції f переходить у вихідну різницю b (операції вважаються зрозумілими з контексту).

Означення 1.3. *Імовірність* $(\circ,\bullet)$*-диференціалу* (a,b) *булевої функції* f (або просто *диференціальна імовірність*) визначається за формулою:

$$DP^f_{\circ,\bullet}(a,b) = \overline{\sum_x}[f(x \circ a) \bullet (f(x))^{-1} = b]$$

Якщо $\bullet \equiv \circ$, то будемо писати просто $DP^f_{\circ}(a,b)$. Також символи використовуваних операцій можуть опускатися, якщо вони є зрозумілими з контексту; в цьому випадку будуть використовуватися позначення $DP^f(a,b)$.

Історично розвиток диференціального криптоаналізу почався з дослідження випадку, коли операції різності на вході та виході співпадають з операцією побітового додавання: $\bullet \equiv \circ \equiv \oplus$. Якщо брати вхідну та вихідну різниці через операцію побітового додавання, то відповідні диференціальні імовірності матимуть наступне значення.

Похідною булевої функції $f(x)$ *за напрямком* a називається функція $D_a f(x) = f(x) \oplus f(x \oplus a)$. Таким чином

$$DP^f_{\oplus\oplus}(a,b) = \overline{\sum_x}[f(x \oplus a) \oplus f(x) = b] = \overline{\sum_x}[D_a f(x) = b],$$

тобто диференціальні імовірності описують розподіли похідних даної булевої функції при випадковому аргументі.

В зарубіжних джерелах для диференціальної імовірності часто використовується позначення $DP(a \xrightarrow{f} b)$ або $DP^f(a \to b)$ (маючи на увазі, що вхідні та вихідні операції беруться за операцією $\oplus$). Таке позначення більш ілюстративне та зручне для опису складних диференціальних переходів.

Означення 1.4. Позначимо через $\delta_f(a,b)$ — *потужність диференціалу* (a,b), тобто кількість x для яких виконується рівність

$$f(x \oplus a) \oplus f(x) = b,$$

тоді *диференціальною рівномірністю функції* f будемо називати таку величину

$$\delta(f) = \max_{a \neq 0, b} \delta_f(a,b).$$

З означення 1.3. також випливає, що $DP^f(a,b) = \frac{\delta_f(a,b)}{2^n}$.

Введемо додаткове позначення

$$MDP_{\circ,\bullet}(f) = \max_{a \neq 0, b} DP^f_{\circ,\bullet}(a\,,b).$$

Наведемо властивості диференціальних імовірностей, які використовуються в диференціальному криптоаналізі. Доведення цих властивостей можна знайти у [1, 2, 3, 4, 5, 7, 8, 9, 10].

Для булевої функції $f : V_n \to V_n$ виконуються такі співвідношення:

$$DP^f(a,b) = [b = 0],$$

$DP^f(a,b) = [b = 0]$, якщо функція f є бієктивною

$$\forall a : \sum_{b \in V_n} DP^f(a,b) = 1,$$

$\forall b : \sum_{a \in V_n} DP^f(a,b) = 1$, якщо функція f є бієктивною

На практиці зручно представляти диференціальні імовірності булевої функції у вигляді спеціальної матриці.

Означення 1.5. *Таблиця розподілів диференціалів* (англ. *difference distribution table*) — матриця розмірності $2^n \times 2^n$, елементами якої є імовірності DP^f. Така матриця позначається як

$$DDT^f = ||DP^f(a,b)||,\ a,b \in V_n.$$

Розглянемо булеву функцію $f_k : V_n \times K \to V_n$, параметризовану ключем. Визначення диференціалу для неї залишається незмінним, однак змінюється визначення диференціальних імовірностей.

Для фіксованого ключа аналітик може розглянути аналогічну попередньо введеній імовірність

$$DP_{\circ,\bullet}[k](a,b) = \overline{\sum_x}[f_k(x \circ a) \bullet (f_k(x))^{-1} = b].$$

Для кожного значення k будуть існувати високоімовірні диференціали, які б можна було використати для проведення атаки. Однак ці диференціали будуть для кожного ключа свої, а тому для проведення успішної атаки аналітику потрібен ключ. Щоб обійти це замкнене коло, для диференціального аналізу використовують такі диференціали, імовірності яких є високими для більшості можливих значень ключів. Для цього замість точних значень диференціальних імовірностей при фіксованих ключах використовують усереднені за ключами диференціальні імовірності.

Означення 1.6. *Середня за ключами імовірність* $(\circ,\bullet)$*-диференціалу* (a,b) *булевої функції* f_k

$$EDP^{f_k}_{\circ,\bullet}(a,b) = \overline{\sum_k} DP^{f_k}_{\circ,\bullet}[k](a,b).$$

Відповідно, вводимо додаткове означення.

Означення 1.7. *Максимальною середньою імовірністю*

$(\circ,\bullet)$-*диференціалу* (a,b) *булевої функції* f_k є

$$MEDP_{\circ,\bullet}(f_k) = \max_{a\neq 0,b} EDP^{f_k}_{\circ,\bullet}(a,b).$$

Також було показано що складність проведення диференціальних атак обернено пропорційна до значення $MEDP$. Таким чином, для оцінки стійкості блокових шифрів до диференціального аналізу потрібно обчислювати або оцінювати зверху максимальні середні імовірності криптографічних перетворень.

На практиці зручними виявились поняття, введені Ковальчук [11].

Означення 1.8. *Середня за ключами імовірність* $(\circ,\bullet)$-*диференціалу* (a,b) *булевої функції* f_k *в точці* x*:*

$$DP^{f_k}_{\circ,\bullet}(x,a,b) = \overline{\sum_k}[f_k(x\circ a)\bullet(f_k(x))^{-1} = b].$$

Відповідний її максимум визначається таким чином:

$$MDP_{\circ,\bullet}(f_k) = \max_{a\neq 0,b,x} DP^{f_k}_{\circ,\bullet}(x,a,b).$$

В силу очевидної нерівності $MEDP_{\circ,\bullet}(f_k) \leq MDP_{\circ,\bullet}(f_k)$ при аналізі стійкості можна оцінювати величину $MDP_{\circ,\bullet}(f_k)$ замість $MEDP_{\circ,\bullet}(f_k)$.

Мають місце такі властивості, доведення яких можна знайти у [11, 12, 13, 14].

Для функції $f_k : V_n \times K \to V_n$ виконуються такі співвідношення:

$$DP^{f_k}(x,0,b) = [b = 0],$$

$$\forall x \forall a : \sum_{b\in V_n} DP^{f_k}(x,a,b) = 1,$$

якщо функція f_k є бієктивною при кожному значенні k, то також виконується

$$DP^{f_k}(x,a,0) = [a = 0],$$

$$\forall x \forall b : \sum_{b \in V_n} DP^{f_k}(x,a,b) = 1.$$

Для відображень, параметризованих ключами, елементами матриці DDT^{f_k} покладемо середні імовірності EDP^{f_k}.

Дуже важливим для диференціального аналізу є поняття марковських перетворень, введене Леєм, Мессі та Мерфі [6].

Означення 1.9. Функція $f_k : V_n \times K \to V_n$ називається *марковським перетворенням (відносно пари операцій* $(\circ,\bullet)$*), якщо значення середніх за ключами диференціальних імовірностей не залежать від точки входу, тобто*

$$\forall x : DP^{f_k}_{\circ,\bullet}(x,a,b) = DP^{f_k}_{\circ,\bullet}(0,a,b),$$

де через 0 позначено нейтральний відносно операції $\circ$ елемент. Якщо ж наведена умова не виконується, будемо казати, що функція f_k є *немарковською відносно операцій* $(\circ,\bullet)$.

Функцію f_k будемо називати *марковською відносно операції* $\circ$, якщо вона є марковським перетворенням відносно пари операцій $(\circ,\circ)$.

З визначення безпосередньо випливає, що для марковського перетворення має місце рівність:

$$\forall x : DP^{f_k}_{\circ,\bullet}(x,a,b) = EDP^{f_k}_{\circ,\bullet}(a,b),$$

а отже, при побудові аналітичних оцінок стійкості до диференціального аналізу можна нехтувати параметром x, фіксуючи його значення довільним зручним чином. Для марковських перетворень мають місце такі властивості [6, 13].

(а) Нехай $f_k : V_n \times K \to V_n$, $g_k : V_n \times K \to V_n$ — марковські перетворення відносно пари операцій $(\circ,\bullet)$. Тоді перетворення $u_{k_1,k_2}(x) = f_{k_1}(x) \bullet g_{k_2}(x)$ також є марковським відносно цих операцій.

(б) Нехай $f_k : V_n \times K \to V_n$ — марковське перетворення відносно пари операцій $(\circ,*)$, а $g_k : V_n \times K \to V_n$ — марковське перетворення відносно пари операцій $(*,\bullet)$. Тоді перетворення $v_{k_1,k_2}(x) = g_{k_2}(f_{k_1}(x))$ є

марковським відносно пари операцій (∘,•). Зокрема, якщо f_k та g_k є марковськими відносно операції ∘ то v_{k_1,k_2} також буде марковським відносно цієї операції.

(в) Нехай $K \equiv V_n$ і функція $f_k : V_n \times K \to V_n$ визначається як $f_k(x) = f(x \circ k)$, де $f : V_n \to V_n$ — деяке безключове перетворення, а ∘ — деяка операція. Тоді для довільної іншої операції • має місце рівність $DP^{f_k}_{\circ,\bullet}(x,a,b) = DP^{f}_{\circ,\bullet}(a,b)$; зокрема, функція f_k є марковською відносно операцій (∘,•).

Використання марковських перетворень для побудови ітеративних шифрів дозволяє будувати аналітичні оцінки стійкості до диференціального аналізу.

1.2 Визначення ітеративного блочного шифру. Теоретична та практична стійкість до диференціального аналізу

Більшість блокових шифрів побудовані як послідовність раундів, де кожен раунд є ключезалежним перетворенням. Ключі, які використовуються в раундах перетворення, називаються раундовими ключами, а ключ що використовується для шифруючого перетворення — ключем шифру. Раундові ключі створюються з ключа шифру за допомогою графіку ключів (англ. key schedule). Блочний шифр з описаною структурою називається ітеративним блочним шифром.

Означення 1.10. *Ітеративний r-раундовий блочний шифр* E — перетворення виду $E : V_n \times K^r \to V_n$, що є композицією r шифруючих перетворень:

$$E = F^{(1)}_{k_1} \circ F^{(2)}_{k_2} \circ ... \circ F^{(r)}_{k_r}.$$

Функції $F^{(i)}_{k_i}$ будемо називати *раундовими перетвореннями*, а змінні k_i — *раундовими ключами*. У диференціальному та лінійному криптоаналізі сучасних блокових шифрів використовують стандартне

модельне модельне припущення, що раундові ключі є випадковими, рівноімовірними та незалежними. Але на практиці ключі не завжди є випадковими і незалежними. Тут і надалі будемо вважати, що раундові ключі $(k_1,k_2,...,k_r)$ є випадковими, незалежними та рівномірно розподіленими в ключовому просторі, якщо не сказано протилежного.

Якщо $Y = E_k(X)$, то пов'яжемо із шифром E та відкритим текстом X послідовність проміжних значень $(X_0,X_1,...,X_r)$, де $X_0 = X$, $X_i = F_{k_i}^{(i)}(X_{i-1})$, $Y = X_r$.

Диференціальний криптоаналіз відноситься до *атак останнього раунду*, так як основною метою проведення даного аналізу є встановлення раундового ключа останнього раунду k_r. Схематично диференціальну криптоатаку на ітеративний блочний шифр можна описати наступним чином.

Нехай на просторі V_n де n — довжина входу, задано дві операції $\times,\bullet$. Розіб'ємо ітеративний шифр у композицію перетворень $E = F_{1,r-1} \circ f_r$, де f_r — останній раунд перетворення E, $F_{1,r-1}$ — всі раунди, окрім останнього. Розглядаються пари відкритих текстів (X,X'), для яких виконується $(X' = X \times a)$ для деякого фіксованого a, та відповідні їм «напівшифротексти» (Y,Y'), де $Y = F_{1,r-1}(X)$, $Y' = F_{1,r-1}(X')$. Припустимо, що криптоаналітику відомо, що для заданого a із високою імовірністю p виконується рівність $Y' = Y \bullet b$ для деякого b (будемо вважати імовірність високою, якщо $p \gg 2^{-n}$). Тоді аналітик може побудувати статистичний розпізнавач для ключа k_r:

1) Аналітик накопичує деяку множину пар випадкових відкритих текстів (X,X') таких, що $X' = X \times a$ та відповідних їм пар шифротекстів (C,C').

2) Для кожного кандидата в ключі k_r аналітик розшифровує пари (C,C') на один раунд та одержує пари (Y,Y').

3) Далі аналітик перевіряє гіпотезу $Y' = Y \bullet b$. Якщо ймовірність цієї події близька до p, то ключ вгадано вірно; якщо ж ймовірність близька до 2^{-n}, то ключ вгадано невірно.

Також аналітик може побудувати структурний розпізнавач: зі значень (C,C') та припущення, що $Y' = Y \bullet b$, аналітик для кожної пари обчислює можливі значення ключа k_r; атака продовжується доти, доки одне зі значень не почне домінувати.

Ключезмінні (англ. key-alternating) блокові шифри це класс ітеративних шифррів, в якому раундові ключі використані дуже простим чином. Далі ключезмінні шифри будемо називати КА-шифрами.

Означення 1.11. КА-шифри — шифри, раундові функції яких мають такий вигляд:

$$F_{k_i}^{(i)}(x) = f(x) \oplus k_i.$$

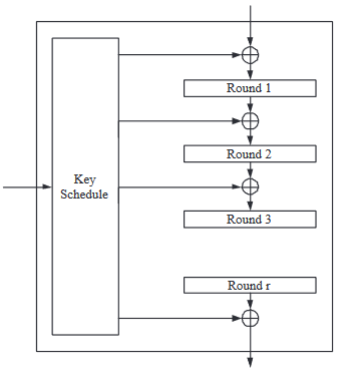

Рисунок 1.1 – Схема ключезмінного шифру

Шифри основані на схемі Фейстеля можна представити як КА-шифри за умови, що функція F є послідовністю додавання раундового ключа та безключового перетворення.

Означення 1.12. Шифр з довгим ключем (англ. long-key cipher) — це КА-шифр у якого ключ шифру має довжину в $h = n(r+1)$ біт, і будується як послідовна конкатенація $r+1$ раундового ключа.

Зауважимо, що шифр з довгим ключем є особливим випадком марковського шифру. А саме, він задовольняє, за означенням, припущення про незалежні та випадкові раундові ключі.

Означення 1.13. *Диференціальна характеристика шифру*

E — послідовність бітових векторів $\Omega = (\omega_0,\omega_1,...,\omega_r)$, де всі $\omega_i \in V_n \backslash \{0\}$.

Диференціальна характеристика розглядається як послідовність змін даних між раундами під час шифрування, тобто якщо подати на вхід два повідомлення X_0 та $X_0^{'}$ такі, що $X_0 \circ (X_0^{'})^{-1} = \omega_0$, то матимемо $X_1 \circ (X_1^{'})^{-1} = \omega_1$, $X_2 \circ (X_2^{'})^{-1} = \omega_2$, ... , $X_r \circ (X_r^{'})^{-1} = \omega_r$. З формальної точки зору диференціальною характеристикою шифру може бути довільна послідовність ненульових двійкових векторів потрібної довжини.

Для характеристики ітеративного шифру величини DP та $\delta_f[k]$ визначаються так само, як і для диференціалів. Як вже було сказано, характеристика це послідовність з r змін (ω_{j-1},ω_j), де кожна така зміна має вагу $w_d(\omega_{j-1},\omega_j)$. Загальну вагу характеристики для шифру з фіксованим ключем ми визначаємо як суму змін з яких вона складається:

$$w_d(\Omega) = \sum_{j=1}^{r} w_d(\omega_{j-1},\omega_j).$$

Означення 1.14. *Середня диференціальна імовірність характеристики* Ω *для шифрів з довгими ключами* визначається наступним чином:

$$DP(\Omega) = \prod_{j} DP(\omega_{j-1},\omega_j).$$

Через $\Omega_{(a,b)}$ ми будемо позначати характеристику, для якої вірно $\omega_0 = a$ та $\omega_r = b$. Очевидно, що потужність диференціалу (a,b) при фіксованому ключі є сумою потужностей всіх характеристик між величинами a та b.

$$\delta[k](a,b) = \sum_{\Omega_{(a,b)}} \delta[k](\Omega_{(a,b)}).$$

Звідси випливає загальна потужність диференціалу (a,b):

$$\delta_{tot}(a,b) = \sum_{k} \delta[k](a,b) = \sum_{k} \sum_{\Omega_{(a,b)}} \delta[k](\Omega_{(a,b)}) = \sum_{\Omega_{(a,b)}} \delta_{tot}(\Omega_{(a,b)}).$$

Означення 1.15. *Середня імовірність диференціальної*

характеристики Ω:

$$EDP^E(\Omega) = \overline{\sum_X} DP^E(\Omega,X).$$

В сучасній теорії [15, 16] розрізняють теоретичну та практичну стійкість диференціального аналізу. Блочний шифр є *теоретично стійким до диференціального аналізу*, якщо виконується нерівність

$$MEDP(E) \leq 2^{-c}$$

для деякого порогового значення c. Блочний шифр є *практично стійким до диференціального аналізу*, якщо виконується нерівність

$$\max_\Omega EDP^E(\Omega) \leq 2^{-c}$$

для деякого порогового значення c.

Теоретична стійкість показує, що складність проведення диференціальної атаки із використанням багатораундових диференціалів в середньому складатиме щонайменше 2^c операцій, а практична стійкість — що складність проведення диференціальної атаки із використанням невеликої кількості диференціальних характеристик складатиме щонайменше 2^c операцій. Практична стійкість шифру гарантує захист від найпоширенішого та (на наш час) самого потужного методу проведення диференціального аналізу, однак не гарантує стійкості в цілому. Втім, оскільки атака із використанням диференціальних характеристик є відносно легкою в проведенні, обидва параметри (як теоретичної, так і практичної стійкості) є важливими.

1.3 Основи лінійного криптоаналізу

Лінійний криптоаналіз являє собою загальний вид криптоаналізу, що використовує лінійні наближення для роботи шифру. Лінійний

криптоаналіз був винайдений японським криптологом Міцуру Мацуі. Алгоритм був спрямований на розкриття FEAL та DES.

Нехай $Y = E_K(X)$ шифруюче перетворення.

Означення 1.16. *Лінійна апроксимація* — трійка векторів (α,β,γ) для якої виконується співвідношення

$$\alpha X \oplus \beta Y \oplus \gamma K = \text{const}.$$

Для шифрів наявність лінійної апроксимації є поганою властивістю, тому її намагаються уникати. Але вона може виникнути з певною імовірністю. Нехай $\Pr_x\{\alpha X \oplus \beta Y \oplus \gamma K = 0\} = p$. Маємо 3 випадки:

$$\text{при } p > 1/2 : \gamma K = \alpha X \oplus \beta Y - \text{домінуюче значення.}$$
$$\text{при } p < 1/2 : \gamma K = \alpha X \oplus \beta Y \oplus 1 - \text{домінуюче значення,}$$
$$\text{при } p = 1/2 \text{ маємо випадок кореляційного імунітету.}$$

Нехай $b \in \{0,1\}$ — випадкова величина з розподілом Бернулі, $\Pr\{b = 1\} = p$. Маємо $p = \frac{1}{2} + s = \frac{1-\epsilon}{2}$, де

$$s \in \left[-\frac{1}{2}; \frac{1}{2}\right] - \text{відхилення,}$$
$$\epsilon \in [-1;1] - \text{кореляція.}$$

Також є вірним $\epsilon = 1 - 2p = Pr\{b = 0\} - Pr\{b = 1\}$.

Для кореляції є істинним таке твердження. Нехай X_1, X_2, ... , X_n — незалежні випадкові величини з розподілом Бернулі, ϵ_i — кореляція X_i. Тоді $X = X_1 \oplus X_2 \oplus ... \oplus X_n$ — випадкова величина із розподілу Бернулі із кореляцією $\epsilon = \prod_{i=1}^{n} \epsilon_i$. З цього випливає, що можна будувати лінійні апроксимації ітеративного шифру шляхом комбінування лінійних апроксимацій на кожному раунді, і їх кореляція буде відома.

Означення 1.17. Нехай функція $F : V_n \to V_n$. *Коефіцієнт Уолша*

функції F:

$$\lambda_F(a,b) = \sum_{x \in V_n} (-1)^{b \cdot F(x) + a \cdot x}.$$

Означення 1.18. *Лінійність* функції F:

$$\mathcal{L}(F) = \max_{a,b \in V_n, b \neq 0} |\lambda_F(a,b)|.$$

Лінійність відповідає зміщенню найкращого лінійного співвідношення між входом і виходом функції F:

$$\Pr_x\{b \cdot F(x) + a \cdot X = 1\} = \frac{1}{2^n}\left(2^{n-1} - \frac{1}{2}\sum_{x \in V_n}(-1)^{b \cdot F(x) + a \cdot x}\right) = \frac{1}{2}\left(1 - \frac{\lambda_F(a,b)}{2^n}\right).$$

Для функції $F : V_n \to V_n$ кореляція приймає значення $\frac{\lambda_F(a,b)}{2^n}$.

Означення 1.19. *Лінійний потенціал* функції F

$$LP^F(a,b) = \left(\frac{\lambda_F(a,b)}{2^n}\right)^2 = (C_F(a,b))^2.$$

Відповідно, *максимальний лінійний потенціал* функції F

$$MLP(F) = \max_{a,b \neq 0} LP^F(a,b).$$

Між значеннями лінійних потенціалів та значеннями диференціальних імовірностей існує зв'язок, про це нам говорить теорема[17].

Теорема 1.1. *Мають місце такі співвідношення:*

$$LP^F(\alpha,\beta) = \frac{1}{2^n}\sum_{a,b \in V_n} (-1)^{\alpha a \oplus \beta b} DP^F_{\oplus}(a,b),$$

$$DP^F_{\oplus}(\alpha,\beta) = \frac{1}{2^n}\sum_{a,b \in V_n} (-1)^{\alpha a \oplus \beta b} LP^F(a,b).$$

Розглянемо функцію $F : V_n \times K \to V_n$, $K = V_l$. Для того щоб коректно оцінювати ключезалежні перетворення необхідно розглядати усереднені по

ключам значення.

Означення 1.20. *Середній за ключами лінійний потенціал* функції F_k визначається таким чином

$$ELP^{F_k}(a,b) = \overline{\sum_k} LP^{F_k}(a,b).$$

Введемо додаткове означення.

Означення 1.21. *Максимальний середній за ключами лінійний потенціал* функції F_k

$$MELP(F_k) = \max_{a,b\neq 0} ELP^{F_k}(a,b).$$

Якщо $F_k(x)$ перетворення виду $S(x \oplus k)$, то для лінійних потенціалів вірно: $\forall a,b\ ELP^{F_k}(a,b) = LP^S(a,b)$.

Якщо $F(x) = G(H(x))$, то коефіцієнт кореляції функції F обраховується таким чином $C_F(a,b) = \sum_\gamma C_H(a,\gamma) \cdot C_G(\gamma,b)$.

1.4 Властивості диференціальних імовірностей та лінійних потенціалів ітеративних відображень

Розглянемо властивості та поведінку диференціальних імовірностей та лінійних потенціалів для перетворень які мають структуру ітеративного блокового шифру з випадковими або невипадковими ключами.

В своїх роботах [18, 19] Рюмен та Демен дослідили асимптотичний розподіл імовірностей $(\oplus,\oplus)$-диференціалів, які індукуються ключем, та показали, що значення EDP будуть параметрами відповідних граничних розподілів. Таким чином, через відомі значення EDP можна будувати аналітичні оцінки для імовірності успіху диференціальних атак та необхідної кількості статистичного матеріалу для проведення цих атак.

Наведемо основні результати їх дослідження.

$$EDP(a,b) = \sum_{\Omega_{(a,b)}} EDP(\Omega_{(a,b)}) = \sum_{\Omega_{(a,b)}} 2^{-w_d(\Omega_{(a,b)})}.$$

$$ELP(a,b) = \sum_{\Omega_{(a,b)}} ELP(\Omega_{(a,b)}).$$

Теорема 1.2. *Для KA-шифрів потужність характеристики з фіксованим ключем та вагою z є стохастичною змінною з таким розподілом:*

$$\Pr\{\delta[k](\Omega) = i\} \approx Poisson(i;\ 2^{n-1-z}) = Poisson(i;\ 2^{n-1}EDP(\Omega)),$$

де функція розподілу вимірює імовірність по всім можливим значенням ключа та по всім можливим графікам ключа.

Теорема 1.3. *Для KA-шифрів загальна потужність диференціалу є стохастичною змінною з таким розподілом:*

$$\Pr\{\delta_{tot}(a,b) = i\} \approx Poisson(i;\ 2^{h+n-1}EDP(a,b)),$$

де функція розподілу вимірює імовірність по всім можливим значенням графіка ключа.

Теорема 1.4. *Якщо кількість лінійних характеристик між величинами a та b велика, то величина $LP[k](a,b)$ є стохастичною змінною з таким Гамма розподілом*

$$\Pr\{LP[k](a,b) = z\} \approx \frac{1}{\sqrt{ELP(a,b)}} \frac{1}{\sqrt{2\pi z}} \exp\left(-\frac{z}{2ELP(a,b)}\right),$$

при $z > 0$, та 0 у іншому випадку. Цей розподіл взятий по всім можливим значенням ключа, і має математичне очікування $ELP(a,b)$ та дисперсію $\sqrt{2}ELP(a,b)$.

В підсумку своїх робіт Рюмен та Демен стверджують, що середнє значення $DP(\delta_{tot})$ характеристики шифру з довгим ключем є таким самим

як і результат отриманий в теорії марковських шифрів. Теорія марковських шифрів також працює для середніх значень $DP(\delta_{tot})$ диференціалів для шифрів з довгим ключем, і з теорією надійності проти диференціальних атак.

В більшості шифрів, які використовуються на практиці, потужність характеристики та диференціалу залежить від значення ключа. Теорема 1.2. показує як в КА-шифрах EDP характеристик та диференціалів визначає розподіл потужностей характеристик та диференціалів із фіксованим ключем.

Тим часом, Теорема 1.3. означає, що середня DP диференціалу або характеристики має розподіл з математичним очікуванням EDP та дисперсією $2^{-(h+n-1)/2}\sqrt{EDP}$. Це вказує на розподіл, який вузько зосереджений навколо середнього значення.

В свою чергу Лі та Вань [21], а потім і Канто та ін. [20] проводили криптографічний аналіз S-блоків побудованих на основі 3-х раундової схеми Фейстеля з фіксованими ключами та знайшли найкращу диференціальну рівномірність та лінійність.

Надійний блочний шифр має слідувати критерію Шеннона та мати властивості змішування та розсіювання. В більшості випадків, змішування досягається за допомогою блоків підміни, або S-блоків, а розсіювання за допомогою лінійних перетворень. Тому надійність шифру залежить від криптографічних властивостей S-блоків. Наприклад, AES [22] використовує восьмибітові S-блоки, які ґрунтуються на основі перестановок в скінченних полях з 2^8 елементами. Цей S-блок має найменшу відому диференціальну імовірність та лінійну кореляцію, що дозволяє AES бути надійним з малою кількістю раундів, та досягати дуже хороших результатів. Але це не завжди найкращий варіант для обмеженого середовища. В якості заміни, були придумані шифри, які використовують чотирьохбітові S-блоки. Але, зменшення кількості змінних збільшує значення оптимальної диференціальної імовірності та лінійної кореляції. Тому необхідно більше раундів для досягнення такої

самої стійкості проти диференціальних та лінійних атак.

Фейстель-подібні структури інтенсивно вивчались в контексті блокових шифрів, і для них були знайдені границі для максимальної очікуваної імовірності диференціалу($MEDP$) та максимального очікуваного лінійного потенціалу ($MELP$).

Дослідження були зосереджені на S-блоках, які мають однакову довжину входу і виходу. Стійкість S-блоку до диференціальних та лінійних атак визначається максимальним значенням в таблиці диференціалів (відп. таблиці лінійних зміщень). Дані параметри вище були введені як диференціальна імовірність та лінійність.

Схема Фейстеля добре відома структура для створення $2n$-бітової перестановки за допомогою менших n-бітових функцій. Функція, що виникає в результаті схеми Фейстеля, завжди є зворотною.

Оскільки Фейстель-подібні структури були використані як основа, при створенні багатьох блокових шифрів, їхні властивості безпеки також інтенсивно вивчались. Натуральним шляхом виміру стійкості створених блокових шифрів до диференціального та лінійного криптоаналізу є вивчення імовірностей диференціалу (відп. потенціалів лінійних наближень) усереднених по всім ключам, тобто $MEDP$ (відп. $MELP$).

Наступна теорема показує нам, що значення $MEDP$ та $MELP$ для мережі Фейстеля можуть бути пов'язані.

Теорема 1.5. *Дано S_1, S_2 та S_3 три n-бітні перестановки, нехай $p = \max_i \delta(S_i)/2^n$ та $q = \max_i(\mathcal{L}(S_i)/2^n)^2$. Тоді для сімейства функцій $(F_K)_{K=(K_1,K_2,K_3)\in GF_2^{3k}}$, визначеного трьома раундами схеми Фейстеля з S_i в якості внутрішніх функцій, виконується*

$$MEDP(F_K) \leq p^2 \text{ та } MELP(F_K) \leq q^2.$$

Дана теорема є дуже значною для побудови ітеративних блокових шифрів: вона показує, що великі функції з сильними криптографічними властивостями можуть бути побудовані з малих функції з сильними

криптографічними властивостями. Для фіксованих значень (a,b) теорема 1.4. доводить, що середні значення $\delta_{F_K}(a,b)$ та $\lambda_{F_K}(a,b)$ є пов'язаними, звідки існує хоча б один ключ, для якого значення не є більшим, ніж середнє. Однак може бути, що значення a,b за яких був досягнутий максимум не є однаковими для кожного ключа.

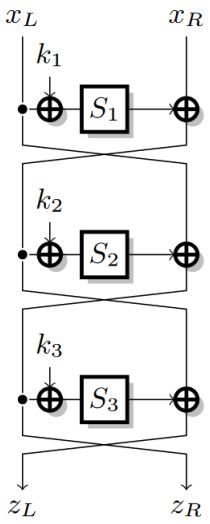

Рисунок 1.2 – 3-х раундова схема Фейстеля

На рисунку 1.2 зображено стандартні 3 раунди шифрування схемою Фейстеля. У своїй роботі Лі та Вань розглядали схему Фестеля з фіксованими ключами, що є еквівалентом даної схеми без ключів, але з різними S-блоками. Дійсно, використання S-блоку S_i з раундовим ключем k_i еквівалентно використанню $S_i^{'} : x \mapsto S_i(x + k_i)$ як S-блоку без ключа.

У своєму дослідженні схеми Фейстеля з фіксованими ключами, Лі та Вань вивели найкращу диференціальну рівномірність та лінійність, яка може бути досягнена трьома раундами шифрування на схемі Фейстеля з константними ключами, тобто ключами із максимально нерівномірними розподілами, та надали приклади які досягають знайдених границь. Їх результати вилились у наступну теорему.

Теорема 1.6. *Нехай S_1, S_2 та S_3 — три n-бітних S-блока та F*

$2n$-бітна функція, визначена відповідною 3-x раундовою схемою Фейстеля. Тоді диференціальна рівномірність $\delta(F) \geq 2\delta(S_2)$. Тим більше, якщо S_2 не є перестановкою, то $\delta(F) \geq 2^{n+1}$. Якщо $n = 4$, для функції F виконується твердження $\delta(F) \geq 8$. Якщо має місце рівність, то лінійність $\mathcal{L}(F) \geq 64$.

Скориставшись, отриманими Лі та Ванем границями, Канто та ін. вивели нижні границі для диференціальної рівномірності та лінійності для 3-х раундів схеми Фейстеля. Для цього спочатку введемо дві нові величини: $\mathcal{L}_{min}$ — найменша лінійність, яку можна отримати для нетривіальної компоненти S-блоку. Подібно до лінійності, δ_{min} — найменше значення, яке можна отримати для $\max\limits_{b} \delta(a,b)$ в середині рядка таблиці диференціалів. Зокрема, для будь-якої чотирьохбітної функції S, $\mathcal{L}_{min} \geq 4$ та $\delta_{min} \geq 2$. Тим паче, якщо S чотирьохбітна перестановка, тоді $\mathcal{L}_{min} \geq 8$ та $\delta_{min} \geq 4$.

Для схеми Фейстеля з S-блоками S_1, S_2 та S_3 було отримано:

– $\delta(F) \geq \delta(S_2) \max(\delta_{min}(S_1), \delta_{min}(S_3))$.

– якщо S_2 не є перестановкою, $\delta(F) \geq 2^{n+1}$.

– $\delta(F) \geq \max\limits_{i\neq 2,\ j\neq i,2}(\delta(S_i)\delta_{min}(S_j),\ \delta(S_i)\delta_{min}(S_2^{-1}))$, якщо S_2 є перестановкою.

– $\mathcal{L}(F) \geq \mathcal{L}(S_2) \max(\mathcal{L}_{min}(S_1), \mathcal{L}_{min}(S_3))$.

– $\mathcal{L}(F) \geq \max\limits_{i\neq 2,\ j\neq i,2}(\mathcal{L}(S_i)\mathcal{L}_{min}(S_j),\ \mathcal{L}(S_i)\mathcal{L}_{min}(S_2^{-1}))$, якщо S_2 є перестановкою.

Результатом роботи Канто також є твердження, що для будь-якого фіксованого ключа існує диференціальна імовірність значення якої більше за значення $MEDP$.

Висновки до розділу 1

У даному розділі були розглянуті основні та необхідні для нашого дослідження теоретичні відомості з диференціального криптоаналізу, а

також основні положення лінійного криптоаналізу. Було розглянуто джерела, в яких досліджувались властивості диференціальних імовірностей та лінійних потенціалів ітеративних відображень.

2 ПОВЕДІНКА ДИФЕРЕНЦІАЛІВ ІТЕРАТИВНИХ ДВОРАУНДОВИХ ПЕРЕТВОРЕНЬ ІЗ ЗАЛЕЖНИМИ КЛЮЧАМИ

У даному розділі буде досліджено, як впливає залежність між раундовими ключами на поведінку імовірностей диференціалів ітеративного шифру, на прикладі крайової ситуації, коли раундові ключі повністю співпадають, а також у випадках, коли наступний раундовий ключ є циклічним зсувом попереднього раундового ключа.

2.1 Опис та постановка задачі

Класичним модельним припущенням у криптоаналізі ітеративних блокових шифрів є випадковість, незалежність та рівноімовірність раундових ключів. Однак для більшості сучасних шифрів схеми генерування раундових ключів не гарантують ані випадковість, ані незалежність раундових ключів. Наприклад, в AES [22] наступні раундові ключі є складними перетвореннями від попередніх, а в шифрі «Калина» [23] ключі непарних раундів є простими циклічними зсувами ключів парних раундів.

Метою цієї роботи є дослідити, як впливає така залежність на поведінку імовірностей диференціалів ітеративного шифру, на прикладі крайової ситуації, коли раундові ключі повністю співпадають, а також у випадках, коли наступний раундовий ключ є циклічним зсувом попереднього раундового ключа.

Для цього, за допомогою таблиць розподілів диференціалів, проведемо порівняльний аналіз диференціальних властивостей двораундових перетворень: $G_k(x) = F_k(F_k(x))$ (з однаковими раундовими ключами), $H_{k_1,k_2}(x) = F_{k_2}(F_{k_1}(x))$ (із двома незалежними раундовими

ключами) та $R_k[l](x) = F_{\rho(k)}(F_k(x))$ (другий раундовий ключ є циклічним лінійним зсув від попереднього), а також порівняння властивостей цих перетворень з властивостями одного раунду $F_k(x)$. В контексті даної роботи величина l буде вказувати на скільки бітів був проведений циклічний зсув вправо, та приймати значення від 1 до 3. У якості раундових функцій ми будемо розглядати типову конструкцію «замішування із ключем + нелінійне перетворення»; три традиційні форми такого раунду позначимо так:

1) $F_k^{(1)}(x) = S(x \oplus k)$;
2) $F_k^{(2)}(x) = S(x) \oplus k$;
3) $F_k^{(3)}(x) = S(x \oplus k) \oplus k$.

Відповідно, верхні індекси у функцій G, H та R позначатимуть, яку форму раундового перетворення було використано.

У якості нелінійного перетворення S будуть розглядатися восьмибітові S-блоки: S-блок шифру AES, чотири S-блоки шифру «Калина», другий S-блок шифру Aria [24], S-блок шифру «Кузнєчік» [25] та S-блок шифру STB [26].

Для імовірностей диференціалів відображень, які розглядаються, мають місце аналітичні співвідношення. Оскільки усі функції $F_k^{(i)}$ та $H_{k_1,k_2}^{(i)}$, $i = \overline{1,3}$, є марковськими перетвореннями, то для них є істинною лема.

Лема 2.1. *Мають місце такі співвідношення:*
– $DDT^{F_k^{(i)}} = DDT^S$;
– $DDT^{H_{k_1,k_2}} = DDT^S \times DDT^S$.

Доведення. Розглянемо функцію $F_k^{(1)}$, за означенням маємо:

$$DP^{F_k^{(1)}}(x,a,b) = \overline{\sum_k}[F_k^{(1)}(x \oplus a) = F_k^{(1)}(x) \oplus b] =$$

$= \overline{\sum_k}[S(x \oplus a \oplus k) = S(x \oplus k) \oplus b]$. Зробимо заміну $u = x \oplus k$. Маємо:

$\overline{\sum_k}[S(u \oplus a) = S(u) \oplus b] = DP^S(a,b)$, що і треба було довести.

Для функції $F_k^{(2)}$ маємо:

$$DP^{F_k^{(2)}}(x,a,b) = \overline{\sum_k}[F_k^{(2)}(x \oplus a) = F_k^{(2)}(x) \oplus b] =$$
$$= \overline{\sum_k}[S(x \oplus a) \oplus k = S(x) \oplus b \oplus k] =$$
$$= \overline{\sum_k}[S(x \oplus a) = S(x) \oplus b] = DP^S(a,b), \text{ що і треба було довести.}$$

Для функції $F_k^{(3)}$ маємо:

$$DP^{F_k^{(3)}}(x,a,b) = \overline{\sum_k}[F_k^{(3)}(x \oplus a) = F_k^{(3)}(x) \oplus b] =$$
$$= \overline{\sum_k}[S(x \oplus a \oplus k) \oplus k = S(x \oplus k) \oplus b \oplus k] =$$
$$= \overline{\sum_k}[S(x \oplus a \oplus k) = S(x \oplus k) \oplus b]. \text{ Зробимо заміну } u = x \oplus k. \text{ Маємо:}$$
$$\overline{\sum_k}[S(u \oplus a) = S(u) \oplus b] = DP^S(a,b), \text{ що і треба було довести.}$$

Для будь-якої функції $F_k^{(i)}$ виконується:

$$DP^{H_{k_1,k_2}}(x,a,b) = \overline{\sum_\gamma} DP^{F_{k_1}^{(i)}}(x,a,\gamma) \cdot DP^{F_{k_2}^{(i)}}(F_{k_1}^{(i)}(x),\gamma,b) =$$
$$= \overline{\sum_\gamma} DP^S(a,\gamma) \cdot DP^S(\gamma,b). \text{ Звідси маємо}$$
$$DDT^{H_{k_1,k_2}} = DDT^S \times DDT^S, \text{ що і треба було довести.}$$

□

2.2 Аналіз результатів дослідження

В ході роботи, для функцій G_k, H_{k_1,k_2}, R_k були розглянуті всі випадки в залежності від раундової функції $F_k^{(i)}$, $i = \overline{1,3}$. Було доведено, що для всіх функцій $F_k^{(i)}$ при фіксованому S-блоці матриці DDT^F є ідентичними, звідки випливає, що матриці DDT^H також будуть ідентичними. Дане твердження випливає із доведення, описаного в кінці підрозділу 2.1 та означення таблиці розподілів диференціалів.

Під час побудови таблиць розподілів диференціалів експериментальним чином було встановлено, що функції G_k та $R_k[l]$ є немарковськими перетвореннями. Шляхом безпосередніх обчислень імовірностей диференціалів в різних точках x для функції $F_k^{(1)}$ та другого

S-блоку «Калини» було отримано:

$$DP^{G_k}(00000000,00001101,00010101) = 1/2^8,$$
$$DP^{G_k}(00000001,00001101,00010101) = 2/2^8,$$

що суперечить означенню марковського перетворення.

Таким самим чином для функції $F_k^{(3)}$ та першого S-блоку «Калини» було отримано:

$$DP^{R_k[2]}(00000000,00001101,00010101) = 2/2^8,$$
$$DP^{R_k[2]}(00000001,00001101,00010101) = 0/2^8,$$

що свідчить про немарковість перетворення $R_k[l]$.

Також, проведені обчислення показали, що для раундових функцій $F_k^{(1)}$ та $F_k^{(2)}$ таблиці DDT^G та DDT^H є ідентичними. Для тих самих функцій $F_k^{(1)}$ та $F_k^{(2)}$ таблиці $DDT^{R_k^{(1)}[l]}$ та $DDT^{R_k^{(2)}[l]}$ співпали з таблицею DDT^H при всіх можливих значеннях величини l. Розрахунки також показали, що для функції $F_k^{(2)}$ таблиці розподілів диференціалів $DDT^{R_k^{(3)}[1]}$ та $DDT^{R_k^{(3)}[3]}$ співпадають між собою.

В результаті порівняльного аналізу диференціальних властивостей двораундових перетворень, які були описані вище, а також одноraундових перетворень для усіх зазначених S-блоків були знайдені наступні величини:

– $MEDP$ — максимальна середня диференціальна імовірність;

– $MELP$ — максимальний середній лінійний потенціал;

– $\#\ \uparrow$ — кількість диференціалів (a,b), імовірність яких збільшилась;

– $\#\ \downarrow$ — кількість диференціалів (a,b), імовірність яких зменшилась;

– $\#\ =$ — кількість диференціалів (a,b), імовірність яких залишилась незмінною;

– $\max\ \uparrow$ — максимальне збільшення імовірності диференціалу;

– $\max\ \downarrow$ — максимальне зменшення імовірності диференціалу.

Також, для немарковських функцій було обраховане значення MDP — максимальної середньої за ключами імовірності диференціалу.

Таблиця 2.1 – Значення величини $2^8 \cdot MEDP$ для функцій $F_k^{(i)}$, $G_k^{(i)}$, $R_k^{(i)}[l]$ та $H_{k_1,k_2}^{(i)}$, $i = \overline{1,3}$, $l = \overline{1,3}$

S-блок	$F_k^{(i)}$	$G_k^{(1)}$, $G_k^{(2)}$	$G_k^{(3)}$	$H_{k_1,k_2}^{(i)}$	$R_k^{(1)}[l]$, $R_k^{(2)}[l]$	$R_k^{(3)}[1]$, $R_k^{(3)}[3]$	$R_k^{(3)}[2]$
AES	4	1,297	18	1,297	1,297	1,5	1,812
Калина 1	8	1,453	10	1,453	1,453	1,656	1,781
Калина 2	8	1,406	12	1,406	1,406	1,547	2
Калина 3	8	1,422	12	1,422	1,422	1,547	1,875
Калина 4	8	1,422	10	1,422	1,422	1,531	1,875
Кузнєчік	8	1,562	12	1,562	1,562	1,719	1,906
STB	8	1,547	10	1,547	1,547	1,656	1,938
Aria	4	1,281	10	1,281	1,281	1,516	1,812

У таблиці 2.1 показано, як змінюється максимальна середня імовірність диференціалу в залежності від перетворення та обраного S-блоку. Як можна бачити $MEDP$ для S-блоків AES та Aria співпадають або майже співпадають для всіх перетворень окрім $G_k^{(3)}$. Для всіх інших S-блоків значення $MEDP$ близькі один до одного і відрізняються від значень для S-блоків AES та Aria. Лише для перетворень $R_k^{(3)}[l]$ імовірності диференціалів є схожими для всіх S-блоків.

Таблиця 2.2 – Значення величини $MELP$ для функцій $F_k^{(i)}$, $G_k^{(i)}$, $R_k^{(i)}[l]$ та $H_{k_1,k_2}^{(i)}$, $i = \overline{1,3}$, $l = \overline{1,3}$

S-блок	$F_k^{(i)}$	$G_k^{(1)}$, $G_k^{(2)}$	$G_k^{(3)}$	$H_{k_1,k_2}^{(i)}$	$R_k^{(1)}[l]$, $R_k^{(2)}[l]$	$R_k^{(3)}[1]$, $R_k^{(3)}[3]$	$R_k^{(3)}[2]$
AES	0,01563	0,00496	0,06250	0,00496	0,00496	0,00615	0,00813
Калина 1	0,03516	0,00587	0,07056	0,00587	0,00587	0,00644	0,00788
Калина 2	0,03516	0,00590	0,07056	0,00590	0,00590	0,00641	0,00756
Калина 3	0,03516	0,00581	0,07910	0,00581	0,00581	0,00690	0,00746
Калина 4	0,03516	0,00605	0,06250	0,00605	0,00605	0,00669	0,00832
Кузнєчік	0,04785	0,00641	0,07910	0,00641	0,00641	0,00763	0,00843
STB	0,04126	0,00631	0,07910	0,00631	0,00631	0,00671	0,00855
Aria	0,01563	0,00502	0,07910	0,00502	0,00502	0,00643	0,00695

Розглянувши таблиці 2.1 та 2.2 можна побачити, що при фіксованих

S-блоках значення $MELP$ для перетворень $G_k^{(i)}$, $R_k^{(i)}[l]$ та $H_{k_1,k_2}^{(i)}$, $i = \overline{1,2}$, $l = \overline{1,3}$, а також $MELP$ для перетворень $R_k^{(3)}[1]$ та $R_k^{(3)}[3]$ співпадають між собою, так само як і значення $MEDP$ для відповідних функцій. Також ми можемо бачити, що при використанні раундових перетворень $F_k^{(i)}, i = \overline{1,3}$ значення $MELP$ для S-блоків шифру Калини є ідентичними.

Ми явно можемо бачити, що функції $R_k^{(3)}[1]$ та $R_k^{(3)}[3]$ дають нам гірші значення $MEDP$ та $MELP$ в порівнянні зі значеннями функції $H_{k_1,k_2}^{(3)}$, але все ще кращі, ніж значення, які були отримані для функції $R_k^{(3)}[2]$. Це говорить нам про те, що для деяких типів раундової функцій та для деяких лінійних перетворень оцінка стійкості виходить гіршою ніж в модельних розрахунках, при чому, для різних функцій оцінка стійкості може бути не однаково гіршою.

Таблиця 2.3 – Значення величини $2^8 \cdot MDP$ для немарковських функцій $G_k^{(i)}$ та $R_k^{(i)}[l]$, $i = \overline{1,3}$, $l = \overline{1,3}$

S-блок	$F_k^{(i)}$	$G_k^{(1)}$	$R_k^{(1)}[1]$	$R_k^{(1)}[2]$	$R_k^{(1)}[3]$	$G_k^{(2)}$	$R_k^{(2)}[1]$	$R_k^{(2)}[2]$	$R_k^{(2)}[3]$
AES	4	9	10	9	10	4	4	4	4
Калина 1	8	10	10	10	9	8	8	8	8
Калина 2	8	9	10	10	9	8	8	8	8
Калина 3	8	9	9	9	11	8	8	8	8
Калина 4	8	10	10	9	10	8	8	8	8
Кузнєчік	8	10	9	9	10	8	8	8	8
STB	8	10	10	9	10	8	8	8	8
Aria	4	10	9	9	10	4	4	4	4
S-блок	$F_k^{(i)}$	$G_k^{(3)}$	$R_k^{(3)}[1]$	$R_k^{(3)}[2]$	$R_k^{(3)}[3]$				
AES	4	18	10	12	12				
Калина 1	4	10	12	10	10				
Калина 2	8	12	10	12	10				
Калина 3	8	12	10	12	12				
Калина 4	8	10	10	10	10				
Кузнєчік	8	12	10	10	10				
STB	8	10	12	10	10				
Aria	4	10	10	10	12				

У таблиці 2.3 ми можемо бачити, що при використанні раундової функції $F_k^{(2)}$ значення MDP при фіксованих S-блоках співпадають для всіх для перетворень $G_k^{(2)}$, $R_k^{(2)}[1]$, $R_k^{(2)}[2]$ та $R_k^{(2)}[3]$, тоді як, при використанні раундових функції $F_k^{()}$ та $F_k^{(3)}$ значення MDP для відповідних перетворень незначно відрізняються. Єдиним винятком є MDP для перетворення $G_k^{(3)}$, яке приймає значення $18/2^8/$

Далі, у таблицях 2.4, 2.5, 2.6, 2.7, 2.8, 2.9 та 2.10 представлені відмінності між DDT^G, DDT^R, DDT^F та DDT^H.

Таблиця 2.4 – Зміни в $DDT^{G_k^{(i)}}$ та $DDT^{R_k^{(i)}[l]}$ відносно $DDT^{F_k^{(i)}}$, $i = 1{,}2$, $l = 1{,}3$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,281	-3,156	32640	32385
Калина 1	1,391	-7,062	36345	28680
Калина 2	1,359	-7,062	36070	28955
Калина 3	1,391	-7,125	36179	28846
Калина 4	1,359	-7,219	36177	28848
Кузнєчік	1,562	-7,203	37725	27300
STB	1,453	-7,359	36980	28045
Aria	1,281	-3,156	32640	32385

З результатів, вказаних у таблиці 2.4, можна зробити наступні висновки. Поведінка S-блоків AES та Aria ідентична і значно відрізняється від усіх інших S-блоків. Для AES та Aria кількість елементів, які збільшились та зменшились, при додатковому раунді шифрування розділилась майже порівну, тоді як для S-блоків «Калини», «Кузнєчіка» та STB кількість елементів, які зросли, більша приблизно на 7 тисяч. Також, відповідно до значень $MEDP$, ми спостерігаємо отримані значення максимального приросту та максимального зменшення.

З таблиці 2.5 ми впевнено можемо сказати, що імовірності диференціалів відображення G для раундової функції типу (3) значно

Таблиця 2.5 – Зміни в $DDT^{G_k^{(3)}}$ відносно $DDT^{F_k^{(3)}}$

S-блок	max $\uparrow \cdot 2^8$	# $=$	# $\uparrow$	# $\downarrow$
AES	16	29516	15828	19681
Калина 1	10	29694	16763	18568
Калина 2	12	29637	16687	18701
Калина 3	12	29857	16511	18657
Калина 4	10	30091	16527	18407
Кузнєчік	10	30083	16999	17943
STB	10	29866	16863	18296
Aria	10	29605	15856	19564

Таблиця 2.6 – Зміни в $DDT^{H_{k_1,k_2}^{(3)}}$ відносно $DDT^{G_k^{(3)}}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,297	-16,969	39317	25708
Калина 1	1,453	-9,109	39225	25800
Калина 2	1,375	-11	39302	25722
Калина 3	1,422	-11	39489	25536
Калина 4	1,422	-9,156	39276	25749
Кузнєчік	1,562	-10,053	39223	25802
STB	1,547	-9,219	39301	25724
Aria	1,281	-9,141	39159	25866

відрізняються від імовірностей диференціалів того самого відображення для раундових функцій типу (1) та (2). На відміну від $DDT^{G_k^{(i)}}$ та $DDT^{R_k^{(i)}[l]}$, $i = 1{,}2$, $l = 1{,}3$, в $DDT^{G_k^{(3)}}$ присутні елементи які не змінились після додаткового раунду шифрування. Також можна зауважити, що всі чисельники елементів матриці $DDT^{G_k^{(3)}}$ є цілими числами. Для кожного розглянутого S-блоку кількості елементів які збільшились, зменшились та залишились незмінними майже однакові, в той час, як максимальний приріст у S-блоку AES помітно відрізняється від інших.

Розглянувши таблицю 2.6 та отримані в ході роботи таблиці розподілів диференціалів можна сказати, що для раундової функції типу

(3) використання відображення G дає нам близько 39 тисяч імовірностей диференціалів, які дорівнюють 0, тоді як за двох раундів шифрування на різних ключах нульові імовірності диференціалів зникають, при чому, для різних диференціалів отримані імовірності незначно відрізняються одна від одної.

Таблиця 2.7 – Зміни в $DDT^{R_k^{(3)}[1]}$ та $DDT^{R_k^{(3)}[3]}$ відносно $DDT^{F_k^{(3)}}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,5	-3,25	32640	32385
Калина 1	1,656	-7,156	36345	28680
Калина 2	1,547	-7,125	36070	28955
Калина 3	1,547	-7,156	36179	28846
Калина 4	1,516	-7,25	36177	28848
Кузнєчік	1,719	-7,266	37725	27300
STB	1656	-7,438	36980	28045
Aria	1,516	-3,25	32640	32385

Таблиця 2.8 – Зміни в $DDT^{H_{k_1,k_2}^{(3)}}$ відносно $DDT^{R_k^{(3)}[1]}$ та $DDT^{R_k^{(3)}[3]}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$	# $=$
AES	0,406	-0,359	30212	30282	4531
Калина 1	0,391	-0,344	30236	30317	4472
Калина 2	0,359	-0,406	30194	30234	4597
Калина 3	0,391	-0,375	30368	30151	4506
Калина 4	0,375	-0,375	30276	30076	4673
Кузнєчік	0,375	-0,469	30073	30344	4608
STB	0,406	-0,422	30098	30286	4641
Aria	1,281	-0,391	30270	30216	4539

Провівши аналіз таблиць 2.7 та 2.8 можна сказати, що перетворення $DDT^{R_k^{(3)}[1]}$ та $DDT^{R_k^{(3)}[3]}$ значно відрізняються від одного раунду функції $F_k^{(3)}$, але не так суттєво відрізняється від перетворення $DDT^{H_{k_1,k_2}^{(3)}}$. У

таблиці 2.8 ми бачимо, що приблизно 4,5 тисячі елементів $DDT^{H^{(3)}_{k_1,k_2}}$ співпадають з елементами таблиць $DDT^{R^{(3)}_k[1]}$ та $DDT^{R^{(3)}_k[3]}$, а всі інші імовірності диференціалів, або збільшились, або зменшились на незначну кількість. Винятком є S-блок шифру Aria, для якого максимальний приріст склав $1{,}281/2^8$.

Таблиця 2.9 – Зміни в $DDT^{R^{(3)}_k[2]}$ відносно $DDT^{F^{(3)}_k}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,178	-3,375	32640	32385
Калина 1	1,178	-7,344	36345	28680
Калина 2	2	-7,062	36070	28955
Калина 3	1,844	-7,438	36179	28846
Калина 4	1,781	-7,281	36177	28848
Кузнєчік	1,906	-7,375	37725	27300
STB	1,938	-7,5	36980	28045
Aria	1,812	-3,375	32640	32385

Таблиця 2.10 – Зміни в $DDT^{H^{(3)}_{k_1,k_2}}$ відносно $DDT^{R^{(3)}_k[2]}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$	# $=$
AES	0,609	-0,828	31731	30561	2733
Калина 1	0,609	-0,641	31534	30761	2730
Калина 2	0,625	-0,844	31601	30740	2684
Калина 3	0,672	-0,688	31677	30734	2614
Калина 4	0,625	-0,688	31529	30910	2586
Кузнєчік	0,595	-0,672	31599	30810	2616
STB	0,609	-0,719	31724	30632	2669
Aria	0,609	-0,719	31518	30847	2660

У таблиці 2.9 ми бачимо що імовірності диференціалів перетворення $R^{(3)}_k[2]$ значно відрізняються від імовірностей одного раунду функції $F^{(3)}_k$.

Всі елементи $DDT^{F_k^{(3)}}$ змінили свої значення при додатковому раунді шифрування на ключі, який був циклічно зсунутий вправо на 2 біти. Для S-блоків шифрів AES та Aria кількість елементів, які збільшились та зменшились, розділилась майже порівну, коли для інших S-блоків різниця між імовірностями диференціалів, які зросли та спали, складає приблизно 7 тисяч.

Таблиця 2.10 показує нам, що відмінності між $DDT^{H^{(3)}_{k_1,k_2}}$ та $DDT^{R_k^{(3)}[2]}$ знову є незначними. Але цього разу, кількість імовірностей диференціалів, які співпадають для двох таблиць розподілів диференціалів, складає 2,5 тисячі, що на 2 тисячі менше ніж для $DDT^{R_k^{(3)}[1]}$ та $DDT^{R_k^{(3)}[3]}$. Також, порівнюючи таблиці 2.8 і 2.10 ми бачимо, що значення максимального приросту та максимального зменшення для перетворення $R_k^{(3)}[2]$ по модулю більші, ніж відповідні значення для перетворень $R_k^{(3)}[1]$ та $R_k^{(3)}[3]$.

Висновки до розділу 2

В даному розділі були описані результати дослідження, метою якого було показати як впливає залежність між раундовими ключами на поведінку диференціалів ітеративного шифру. Для цього були обраховані таблиці розподілів диференціалів для двох та одного раундів шифрування, після чого отримані таблиці були співставлені одна з одною.

Можемо сказати, що використання раундових ключів які, або співпадають, або є залежними один від одного дуже простим чином, суттєво погіршує стійкість до диференціального та лінійного криптоаналізу у порівнянні з ситуацією, коли два ключі є різними та незалежними. Погіршення виникає як і при використанні функцій $R_k^{(3)}[1]$, $R_k^{(3)}[3]$, так і при використанні функції $R_k^{(3)}[2]$ (для функцій $R_k^{(3)}[1]$ та $R_k^{(3)}[3]$ погіршується краще).

Слід зауважити, що в даному розділі розглядались тільки

дворaундові перетворення з простою структурою, тому треба перевіряти чи збережуть $MEDP$ та $MELP$ результати для трьох та більше раундів перетворення або для функцій із більш складною структурою.

У результаті ми можемо стверджувати, що ітеративне перетворення із залежними раундовими ключами втрачає властивість марковості, а тому до нього не може бути застосовна існуюча формальна теорія диференціального криптоаналізу. Однак для деяких форм раундових функцій перетворення з однаковими ключами може зберігати окремі властивості перетворень з незалежними ключами, зокрема, значення середніх імовірностей диференціалів.

ВИСНОВКИ

У даній роботі було проведено огляд відкритих джерел і показано, що поведінка диференціалів та лінійних потенціалів ітеративних двораундових перетворень із залежними раундовими ключами не розглядалось

В роботі було досліджено поведінку диференціалів та лінійних потенціалів ітеративних двораундових перетворень із залежними раундовими ключами для перевірки стандартного модельного припущення у криптоаналізі блокових шифрів про незалежність раундових ключів.

Експериментально було показано, що перетворення із залежними раундовими ключами втрачають властивість марковості, однак для деяких форм раундової функції вони можуть зберігати окремі властивості модельних шифрів – зокрема, значення середніх імовірностей диференціалів. Для деяких перетворень із залежними ключами значення максимальної середньої імовірності диференціалу та максимального середнього лінійного потенціалу збігаються із відповідними значеннями для перетворень із незалежними ключами. Для перетворень з одним циклічним зсувом ключа значення максимальної середньої імовірності диференціалу та максимального середнього лінійного потенціалу можуть бути гіршими ніж для перетворень з іншим циклічним зсувом ключа.

Криптографічні властивості ітеративних перетворень із однаковими або, у більш загальному випадку, залежними раундовими ключами вимагають подальших аналітичних та експериментальних досліджень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Biham E. Differntial cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.

2. Biham E. Differential cryptanalysis of the full 16-round DES / E. Biham, A. Shamir // Advances in Cryptology – CRYPTO'92, Proceedings. – Springer Verlag, 1993. – P. 487 – 496.

3. Chabaud Florent. Links between Differential and Linear Cryptanalysis [електронний ресурс] / Florent Chabaud, Serge Vaudenay. – Режим доступу : http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.48.2675

4. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. – Doctoral Dissertation, 1995.

5. Heys Howard M. A Tutorial on Linear and Differential Cryptanalysis [електронний ресурс] / Howard M. Heys. – Режим доступу : http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

6. Lai Xuejia, Massey James L., Murphy Sean.Markov Ciphers and Differential Cryptanalysis //Advances in Cryptology — EUROCRYPT '91 /Ed. by Donald W. Davies.—Berlin, Heidelberg :Springer Berlin Heidelberg, 1991. — P. 17–38.

7. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis / M. Matsui // IEICE Trans. Fundamentals. – Vol. E82-A. – #1. – 1999. – pp. 117-122.

8. O'Connor L. A unified Markov approach to differential and linear cryptanalysis / L. O'Connor, J.D. Golic // Advances in Cryptology – ASIACRYPT'94, Proceedings. – Springer Verlag, 1994. – P. 387 – 397.

9. Selcuk, A.A. On probability of success in linear and differential cryptanalysis. / A.A. Selcuk // Journal of Cryptology. – Vol. 21(1). – 2008. – pp. 131- 147.

10. Vaudenay S. Decorrelation: a theory for block cipher security / S. Vaudenay // Journal of Cryptology. – 2003. – V. 16. – № 4. – pp. 249-286.

11. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа / Л.В. Ковальчук // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25 – 27 октября 2006 г. – М.: МЦНМО, 2007. – С. 595 – 599.

12. Ковальчук Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу / Л.В. Ковальчук, С.В. Пальченко, Л.В. Скрипник // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – К.: НДЦ «Тезіс», 2009 – №2 (19) – стор. 45-56.

13. Ковальчук Л.В. Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2 / Л.В. Ковальчук, А.О. Шерстюк // Прикладная радиоэлектроника. – №3. – 2009. – С. 15–27.

14. Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. / Л. Ковальчук, Н. Кучинская // Кибернетика и системный анализ. – 2012. – №5. – С. 71-81.

15. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function / M. Kanda // Selected Areas in Cryptography. –SAC 2000, Proceedings. –Springer Verlag, 2001. –P. 324 –338.

16. Knudsen L.R. Practically secure Feistel cipher / L.R. Knudsen// Fast Software Encryption. –FSE'94, Proceedings. –Springer Verlag, 1994. – P. 211 – 221.

17. Vaudenay S. Decorrelation: a theory for block cipher security / S. Vaudenay // Journal of Cryptology. – 2003. – V. 16. – № 4. – pp. 249-286.

18. Daemen Joan, Rijmen Vincent. Probability distributions of correlation and differentials in blockciphers // Journal of Mathematical

Cryptology.—2007. — Vol. 1, no. 3. — P. 221 – 242.

19. Daemen Joan, Rijmen Vincent. Statistics of Correlation and Differentials in Block Ciphers.—2008.—Access mode: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.4898.

20. Canteaut A. Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version) [електронний ресурс] / Anne Canteaut, Sebastien Duval, Gaetan Leurent – 2015. – С. 2-5 - Режим доступу: http://eprint.iacr.org/2015/711.pdf

21. Li Y., Wang M. Constructing S-boxes for Lightweight Cryptography with Feistel Structure //Cryptographic Hardware and Embedded Systems –CHES 2014 / Ed. by Lejla Batina, Matthew Rob-shaw.—Berlin, Heidelberg : Springer Berlin Hei-delberg, 2014. — P. 127–146.

22. FIPS PUB 197 : Advanced Encryption Standard.—2001.

23. Oliynykov Roman, Gorbenko Ivan, Kazymyrov Oleksandr et al. A New Encryption Standardof Ukraine: The Kalyna Block Cipher.—Cryptology ePrint Archive, Report 2015/650.—2015.—https://eprint.iacr.org/2015/650.

24. New Block Cipher: ARIA / Daesung Kwon, Jae-sung Kim, Sangwoo Park et al. // InformationSecurity and Cryptology - ICISC 2003 / Ed. byJong-In Lim, Dong-Hoon Lee.—Berlin, Heidelberg :Springer Berlin Heidelberg, 2004. — P. 432–445.

25. Информационная технология. Криптографическая защита информации. Блочные шифры :ГОСТ 34.12-2018. — 2018.

26. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности : СТБ34.101.31-2011. — 2011.